UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/615,676	07/14/2000	Michael P. Lyle	RECOP005	6964

21912 7590 07/19/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	14

DATE MAILED: 07/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary	**Application No.** 09/615,676	**Applicant(s)** LYLE ET AL.	
	Examiner Matthew Heneghan	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2004 and 20 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21,26-29,31-38 and 41-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21,26-29,31-38 and 41-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *10*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. In response to the first office action, Applicant has amended claims 1, 3, 8, 18, 26, 28, 29, 31-33, and 41-43; and cancelled claims 22-25, 30, 39, and 40. Claims 1-21, 26-29, 31-38, and 41-43 have been examined.

Priority

2. Regarding Applicant's arguments that the claim for domestic priority under 35 U.S.C. 119(e) to Provisional U.S. Patent Application 60/151,531, filed 30 August 1999 is proper because at least one claim in the instant application is enabled, see Paper No. 12, filed 17 May 2004, Applicant's argument is persuasive. The objection to the priority claim is withdrawn.

Information Disclosure Statement

3. The following Information Disclosure Statement in the instant application has been fully considered:

Paper No. 10, filed 29 May 2004.

Drawings

4. The drawings were received on 17 May 2004. These drawings are not acceptable.

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference character mentioned in the description: item "1720" on page 55, line 14. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

6. The previous objections to the specification are withdrawn.

Claim Objections

7. Claim 10 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The additional limitation of claim 10 is wholly contained in base claim 8. For purposes of the prior art search, claim 10 stands or falls with claim 8.

Claim Rejections - 35 USC § 112

8. All previous rejections under 35 U.S.C. 112 are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,499,107 to Gleichauf et al. in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee.

Note: Gleichauf was cited in the previous office action.

Gleichauf monitors successive data sets ("traffic") and identifies attack signatures for various events (see column 6, lines 25-45); the data are assigned to a plurality of groups according to the attack type (see column 6, lines 51-65), and data not associated with a particular group end up in other groups; and prioritizes the groups, such that critical events receive the highest priority for processing (see column 8, lines 35-41).

Gleichauf does not specify how successive entries are organized with respect to one another.

Trcka discloses the servicing of traffic on a first-in-first-out basis (queuing) and further suggests that this allows for a near-real-time representation of events taking place on the network (see column 17, lines 14-23).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the groups disclosed by Gleichauf as queues, as disclosed by Trcka, to allow for a near-real-time representation of events taking place on the network.

Gleichauf and Trcka also do not address the method for servicing different queues having equal priority.

Lee discloses a method for priority arbitration wherein the arbiter carries out a round-robin scheduling process (groups are serviced in turns), and suggests that this ensures that all inputs of equal priority achieve fair access to the resource being arbitrated (see column 1, lines 40-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to further implement the invention of Gleichauf and Trcka by using a round-robin scheduling process for groups having equal priority, as disclosed by Lee, to ensure that all inputs of equal priority achieve fair access.

10. Claims 1-4, 7-11, 20, 21, and 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of U.S. Patent No. 6,499,107 to Gleichauf et al. further in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee.

Regarding claim 1, the network surveillance system disclosed by Conklin monitors intrusion detections.

Conklin does not disclose the method by which incoming events are stored while awaiting processing.

Gleichauf, Trcka, and Lee disclose a method for processing events, as described above, and Gleichauf further suggests that conventional systems, when confronted with traffic that exceeds their capacity, may start dropping packets and degrade performance in an unpredictable fashion (see Gleichauf, column 2, lines 36-39).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the event processor of Conklin by using the method of Gleichauf, Trcka, and Lee, since conventional systems, when confronted with traffic that exceeds their capacity, may start dropping packets and degrade performance in an unpredictable fashion.

As per claims 2-4 and 7-11, the system disclosed by Conklin may respond by automatically sending an alert message to a network management system (which is trusted) using Trap PDUs (see column 5, lines 46-60).

As per claims 20 and 21, the system classifies data by the type of event, processing successive sets of data (see column 6, lines 1-12).

As per claim 31, attack checks are comparative, and different events are therefore associated with one another (see column 7, lines 51-55).

As per claim 32, pattern matching is used, therefore allowing events with the same message to be correlated.

As per claim 33, incoming packets are also correlated with historical data.

As per claim 34, source IP addresses are reported (see column 5, lines 29-30).

11. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of U.S. Patent No. 6,499,107 to Gleichauf et al. further in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee as applied to claim 4 above, and further in view of U.S. Patent No. 6,311,274 to Day.

Conklin, Gleichauf, Trcka, and Lee only disclose event notifications via SNMP traps.

The network alert system disclosed by Day includes alert notifications in the event of network intrusions via email or pager (see column 5, lines 33-55), and suggests the necessity of performing an appropriate alert action in response to the alert message.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin, Gleichauf, Trcka, and Lee by implementing an alert system that might send notifications by pager or email, as disclosed by Day, due to the necessity of performing an appropriate alert action in response to the alert message.

12. Claims 12-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of U.S. Patent No. 6,499,107 to Gleichauf et al. further in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee as applied to claim 1 above, and further in view of U.S. Patent No. 6,067,620 to Holden et al.

Regarding claims 12-14, Conklin, Gleichauf, Trcka, and Lee do not disclose the direct monitoring or manipulation of network ingress and egress ports.

The security device disclosed by Holden includes a hardware SNIU, a network interface that is placed on every network interface in a system that is connected to an untrusted network (such as computers, routers, switches, etc.) and diverts incoming data to a set of secure modules to process packets (constituting a copy port). A network of SNIU-equipped machines creates a global security perimeter.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin, Gleichauf, Trcka, and Lee by using the SNIU disclosed by Holden on all network interfaces, in order to create a global security perimeter.

As per claim 15, Conklin discloses internal network communications using SNMP, a network management protocol.

As per claims 16-19, Conklin discloses the scanning of packets for contents (such as strings) and monitors services that are vulnerable, such as telnet (see column 2, line 64 to column 3, line 14).

13. Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,499,107 to Gleichauf et al. in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee as applied to claim 1 above, and further in view of U.S. Patent No. 5,574,912 to Hu et al.

Gleichauf, Trcka, and Lee do not disclose the organization of the queues as a matrix.

The lattice scheduler disclosed by Hu includes places processes within a lattice of queues for processing, with the indices depending upon attributes of the processes being placed, that are then executed in a round-robin manner, with subsequent queues being used when queues are exhausted (see column 8, line 50 to column 9, line 8). Hu further suggests that this is done to achieve better CPU utilization (see column 5, lines 32-35).

Therefore it would been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Gleichauf, Trcka, and Lee by organizing the queues in a matrix, as disclosed by Hu, to achieve better CPU utilization.

14. Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,499,107 to Gleichauf et al. in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee as applied to claim 1 above, and further in view of U.S. Patent No. 5,574,912 to Hu et al. as applied to claim 27 above, and further in view of U.S. Patent No. 6,233,686 to Zenchelsky et al.

Gleichauf, Trcka, Lee, and Hu do not disclose the hashing of string data or IP addresses in order to derive the table indices in which data is to be inserted.

The network access control system of Zenchelsky includes the hashing of network addresses (see abstract), which are IP addresses, or string data (see column 6, line 60 to column 7, line 5) for determining table indices, and suggests that hash tables are used to allow more efficient searching.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Gleichauf, Trcka, Lee, and Hu by organize the matrix of queues as hash tables, using network addresses and/or string contents, as disclosed by Zenchelsky, as hash tables are used to allow more efficient searching.

15. Claims 35-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of U.S. Patent No. 6,499,107 to Gleichauf et al. further in view of U.S. Patent No. 6,453,345 to Trcka et al. further in view of U.S. Patent No. 5,301,333 to Lee as applied to claim 35 above, and further in view of U.S. Patent No. 6,442,694 to Bergman et al.

Conklin, Gleichauf, Trcka, and Lee do not disclose the tracing back to determine the point of attack.

The fault isolation system disclosed by Bergman uses a network map mapping all the nodes in a network, stored at each system, wherein, upon detection of an attack at a node, the attack is iteratively traced back to the point at which it entered the network see column 14, line 59 to column 19, line 20). Bergman further suggests that it would be desirable to provide a technique for localizing an attack on a network (see column 7, lines 55-62).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin, Gleichauf, Trcka, and Lee by using the fault isolation technique disclosed by Bergman to trace back attacks, in order to localize an attack on a network.

Double Patenting

16. In view of Applicant's terminal disclaimer, all previous rejections due to double patenting are withdrawn.

Terminal Disclaimer

17. The terminal disclaimer filed on 20 May 2004 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of

U.S. Patent No. 6,647,400 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Arguments

18. Applicant's arguments, see Paper No. 12, filed 17 May 2004, with respect to the rejections of all the remaining claims under 35 U.S.C. 103 have been fully considered and are persuasive in view of Applicant's amendments. Therefore, the rejections have been withdrawn. However, upon further consideration, new grounds of rejection are made as described above.

Conclusion

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday, Tuesday, Thursday, and Friday from 7:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MEH MEH

July 2, 2004